Published March 23, 2026 · Last revised March 23, 2026

BotmasterLabs: Powering an Era of Spam

bot management · fingerprinting · spam

2026

Table of Contents

1. Executive Summary

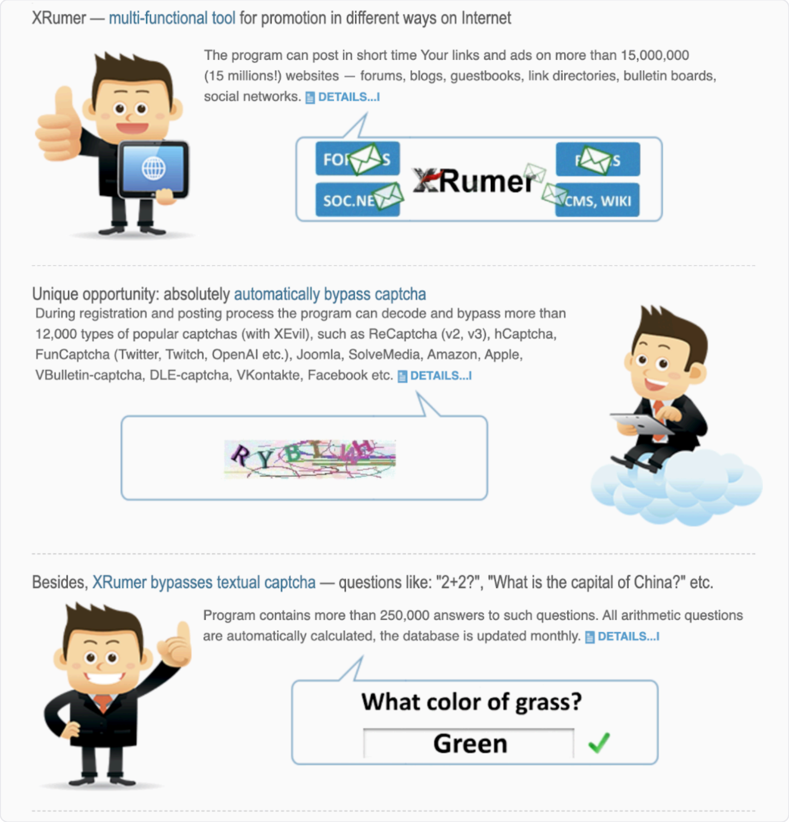
Castle's Research Team continues to monitor the evolving bot landscape, with this report providing a comprehensive analysis of BotmasterLabs, a software company known for developing spam-related tools that have gained adoption in both the Russian and Western cybercrime spaces. BotmasterLabs is known for XRumer, a forum spamming toolkit, and XEvil, a CAPTCHA-solving plug-in, both of which have enabled low-level spam for the past decade. XRumer grants clients the ability to import or select predefined lists of websites to spam with custom messages, and it has been observed being used to push malvertising or pharmaceutical-based advertisements. This software is provided in addition to XEvil and leverages both Optical Character Recognition (OCR) and machine learning models to solve over 100 different text- and image-based CAPTCHAs.

Defenders should use and enforce strict browser fingerprinting techniques and apply additional scrutiny to IPv6 and Datacenter IP ranges. Additionally, organizations should use multiple forms of challenge and not over-rely on a single form of verification; instead, use a holistic analysis of the user beyond a single fingerprint, IP address, or email.

Looking ahead, Castle's Research Team expects continued adoption of third-party tools to power large-scale bot farms and credential-stuffing attacks. XEvil highlights the significant shortcomings of image-based CAPTCHA, suggesting the need for more complex signals.

2. Background

BotmasterLabs is a Russian-speaking actor that has been operating since early 2007, and it is best known for developing XRumer, one of the largest forum-spamming toolkits, and XEvil, a CAPTCHA-solving plugin used for low-level credential stuffing and large-scale account farms. This software has gained popularity due to its low barrier to entry in both cost and skill, making it an easy choice for circumventing traditional security measures. Castle's Research Team continues to track the CAPTCHA and spam ecosystem to protect clients and build stronger client-side fingerprinting signals for automated abuse. This report aims to provide a comprehensive analysis of the techniques, tactics, and procedures (TTPs) used by both tools, with findings highlighting significant shortcomings that enable defenders to detect and mitigate automated abuse.



XRumer — multi-functional tool for promotion in different ways on Internet

The program can post in short time Your links and ads on more than 15,000,000 (15 millions!) websites — forums, blogs, guestbooks, link directories, bulletin boards, social networks. DETAILS...!

Unique opportunity: absolutely automatically bypass captcha

During registration and posting process the program can decode and bypass more than 12,000 types of popular captchas (with XEvil), such as ReCaptcha (v2, v3), hCaptcha, FunCaptcha (Twitter, Twitch, OpenAI etc.), Joomla, SolveMedia, Amazon, Apple, VBulletin-captcha, DLE-captcha, VKontakte, Facebook etc. DETAILS...!

Besides, XRumer bypasses textual captcha — questions like: "2+2?", "What is the capital of China?" etc.

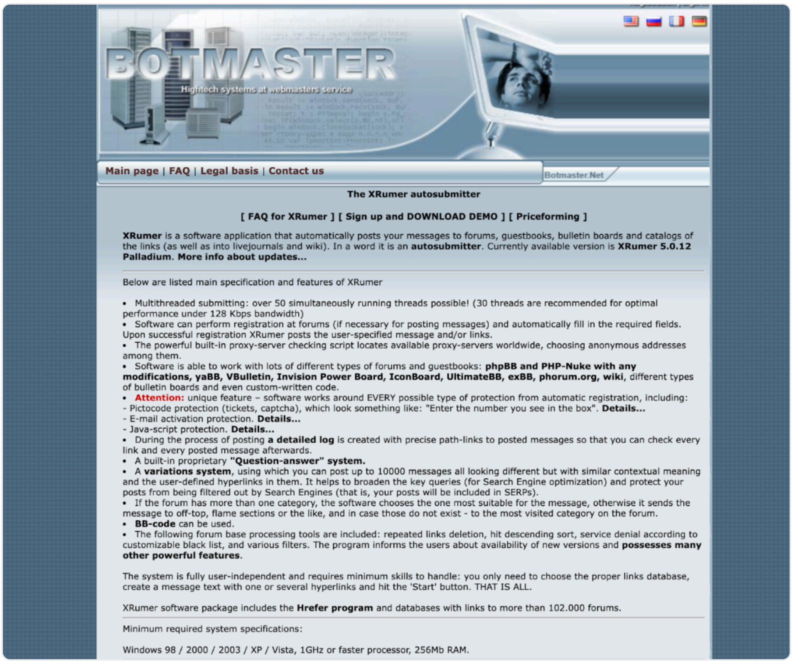
Program contains more than 250,000 answers to such questions. All arithmetic questions are automatically calculated, the database is updated monthly. DETAILS...!

What color of grass?

Green ✓

Fig 01. BotmasterLabs XRumer landing page. (Archive.org)

XRumer is one of the first products offered by BotmasterLabs, marketed as a “link-building tool” that could automatically register accounts on various forum software and promote custom-made messages. XRumer would gain early adoption among spammers, used for a wide range of purposes, from pushing malvertising to running pharmaceutical ads. Since its initial release, the software has undergone significant improvements, with the latest release introducing AI for content generation and form detection, as well as improvements to anti-bot circumvention.



BOTMASTER
Hightech systems at webmasters service
Main page | FAQ | Legal basis | Contact us
Botmaster.Net

The XRumer autosubmitter

[FAQ for XRumer] [Sign up and DOWNLOAD DEMO] [Priceforming]

XRumer is a software application that automatically posts your messages to forums, guestbooks, bulletin boards and catalogs of the links (as well as into livejournals and wiki). In a word it is an **autosubmitter**. Currently available version is **XRumer 5.0.12 Palladium**. **More info about updates...**

Below are listed main specification and features of XRumer

- Multithreaded submitting: over 50 simultaneously running threads possible! (30 threads are recommended for optimal performance under 128 Kbps bandwidth)
- Software can perform registration at forums (if necessary for posting messages) and automatically fill in the required fields. Upon successful registration XRumer posts the user-specified message and/or links.
- The powerful built-in proxy-server checking script locates available proxy-servers worldwide, choosing anonymous addresses among them.
- Software is able to work with lots of different types of forums and guestbooks: **phpBB and PHP-Nuke with any modifications, yaBB, VBulletin, Invision Power Board, IconBoard, UltimateBB, exBB, phorum.org, wiki**, different types of bulletin boards and even custom-written code.
- **Attention:** unique feature – software works around EVERY possible type of protection from automatic registration, including:
  - Pictocode protection (tickets, captcha), which look something like: "Enter the number you see in the box". **Details...**
  - E-mail activation protection. **Details...**
  - Java-script protection. **Details...**
- During the process of posting **a detailed log** is created with precise path-links to posted messages so that you can check every link and every posted message afterwards.
- A built-in proprietary **"Question-answer" system.**
- A **variations system**, using which you can post up to 10000 messages all looking different but with similar contextual meaning and the user-defined hyperlinks in them. It helps to broaden the key queries (for Search Engine optimization) and protect your posts from being filtered out by Search Engines (that is, your posts will be included in SERPs).
- If the forum has more than one category, the software chooses the one most suitable for the message, otherwise it sends the message to off-top, flame sections or the like, and in case those do not exist - to the most visited category on the forum.
- **BB-code** can be used.
- The following forum base processing tools are included: repeated links deletion, hit descending sort, service denial according to customizable black list, and various filters. The program informs the users about availability of new versions and **possesses many other powerful features**.

The system is fully user-independent and requires minimum skills to handle: you only need to choose the proper links database, create a message text with one or several hyperlinks and hit the 'Start' button. THAT IS ALL.

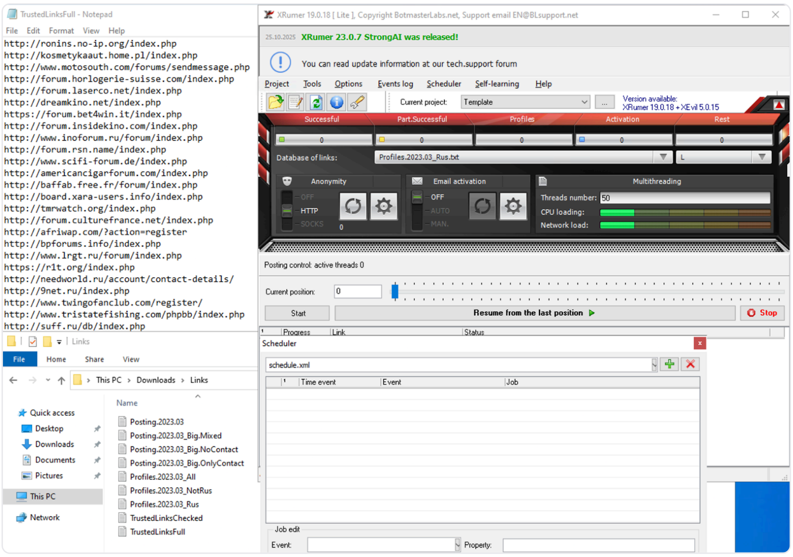
XRumer software package includes the **Hrefer program** and databases with links to more than 102.000 forums.

Minimum required system specifications:

Windows 98 / 2000 / 2003 / XP / Vista, 1GHz or faster processor, 256Mb RAM.

Fig 02. BotmasterLabs 2010 (Archive.org)

In addition to gaining access to the software, BotmasterLabs clients receive ~20 million links to various forums and websites that can be used immediately in XRumer to spam with custom messages. Clients can also use BotmasterLabs HRefer to find new links for forums, guestbooks, blogs, and Wikis.



TrustedLinksFull - Notepad

```
http://ronins.no-ip.org/index.php
http://kosmetykaaut.home.pl/index.php
http://www.motosouth.com/forums/sendmessage.php
http://forum.horlogerie-suisse.com/index.php
http://forum.laserco.net/index.php
http://dreamkino.net/index.php
https://forum.bet4win.it/index.php
http://forum.insidekino.com/index.php
http://www.inoforum.ru/forum/index.php
http://forum.rsn.name/index.php
http://www.scifi-forum.de/index.php
http://americancigarforum.com/index.php
http://baffab.free.fr/forum/index.php
http://board.xara-users.info/index.php
http://tmrwatch.org/index.php
http://forum.culturefrance.net/index.php
http://afriwap.com/?action=register
http://bpforums.info/index.php
http://www.lrgt.ru/forum/index.php
https://r1t.org/index.php
http://needworld.ru/account/contact-details/
http://9net.ru/index.php
http://www.twingofanclub.com/register/
http://www.tristatefishing.com/phpbb/index.php
http://suff.ru/db/index.php
```

This PC > Downloads > Links

- Posting.2023.03
- Posting.2023.03_Big.Mixed
- Posting.2023.03_Big.NoContact
- Posting.2023.03_Big.OnlyContact
- Profiles.2023.03_All
- Profiles.2023.03_NotRus
- Profiles.2023.03_Rus
- TrustedLinksChecked
- TrustedLinksFull

XRumer 19.0.18 [Lite], Copyright BotmasterLabs.net, Support email EN@BLsupport.net

25.10.2025 XRumer 23.0.7 StrongAI was released!

You can read update information at our tech.support forum

Current project: Template

Version available: XRumer 19.0.18 + XEvil 5.0.15

Successful	Part.Successful	Profiles	Activation	Rest
0	0	0	0	0

Database of links: Profiles.2023.03_Rus.txt

Anonymity: HTTP

Email activation: OFF

Threads number: 50

Posting control: active threads 0

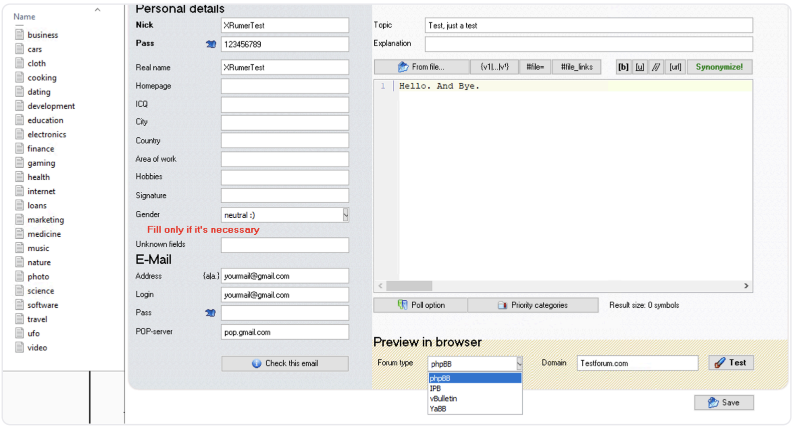
Current position: 0

Scheduler: schedule.xml

Fig 03. XRumer user interface and website lists.

3. XRumer Analysis

XRumer provides a user-friendly graphical interface, allowing users to configure everything from the messages sent to the user details for registered accounts. XRumer provides an additional set of text files containing realistic, random information for use in campaigns. Users can select a specific theme and further fine-tune randomized content around it. Users can also configure proxies, custom rules, scheduling, and self-learning to circumvent bot-protection measures and appear more realistic.



- business
- cars
- cloth
- cooking
- dating
- development
- education
- electronics
- finance
- gaming
- health
- internet
- loans
- marketing
- medicine
- music
- nature
- photo
- science
- software
- travel
- ufo
- video

Personal details

Nick	XRumerTest
Pass	123456789
Real name	XRumerTest
Homepage	
ICQ	
City	
Country	
Area of work	
Hobbies	
Signature	
Gender	neutral :)

Fill only if it's necessary

Unknown fields	

E-Mail

Address	yourmail@gmail.com
Login	yourmail@gmail.com
Pass	
POP-server	pop.gmail.com

Topic: Test, just a test

```
Hello. And Bye.
```

Result size: 0 symbols

Preview in browser

Forum type: phpBB

Domain: Testforum.com

Fig 04. XRumer default headers and health check.

Once a campaign has been started, XRumer creates an isolated session for each forum, pulling auto-fill values from its corpus. Depending on whether the website is a forum or a simple form, it will go through different stages: either automatically filling and submitting the form or following the 6 steps to provision and post with an account.

1. **Guest Browsing**: Fetch website, check if it's available, and set all proper cookies.
2. **Account Registration**: Attempt to sign up by parsing form details and checking the fields against the database of possible form values. Fill in matches and solve the necessary text- and image-based CAPTCHAs.

3. **Authentication**: Follow the redirect flow and log in with credentials. Check the status message to see if registration has been blocked; if not, proceed to phase 4.
4. **Provisioning**: Set up account details such as bios, profile photo, display name, and other characteristics to give the appearance of it being a real account.
5. **Posting**: Mass-DM users on the site or post forum content, depending on the option selected in the campaign.

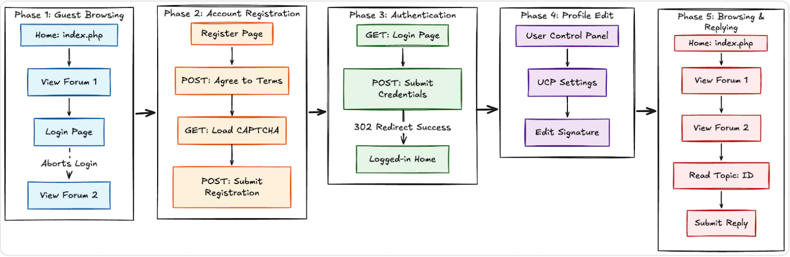
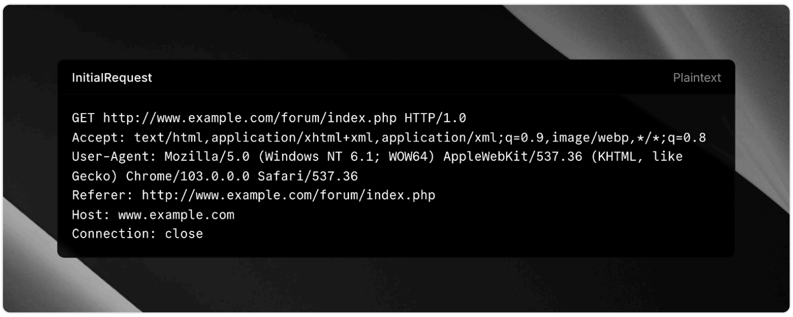


Fig 05. XRumer and its 6 stages for posting on forums.

Castle’s Research Team observed XEvil initializing each session with a randomly selected user agent from the “x_user_agent” file, which contains only 31 user agents pretending to be Windows and Chromium 103.

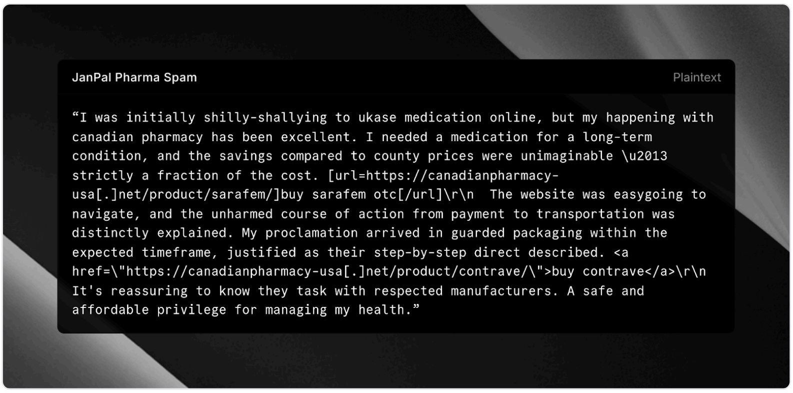


```
GET http://www.example.com/forum/index.php HTTP/1.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.0.0 Safari/537.36
Referer: http://www.example.com/forum/index.php
Host: www.example.com
Connection: close
```

Fig 06. XRumer default headers and health check.

Spammers' Best Friend

Castle’s Research Team purchased an expired domain from the distributed spam list provided to XRumer clients and, within the hour, observed attempts to register and post pharmaceutical-related spam to the message board.



```
“I was initially shilly-shallying to ukase medication online, but my happening with
canadian pharmacy has been excellent. I needed a medication for a long-term
condition, and the savings compared to county prices were unimaginable \u2013
strictly a fraction of the cost. [url=https://canadianpharmacy-
usa[.]net/product/sarafem/]buy sarafem otc[/url]\r\n  The website was easygoing to
navigate, and the unharmed course of action from payment to transportation was
distinctly explained. My proclamation arrived in guarded packaging within the
expected timeframe, justified as their step-by-step direct described. <a
href=\"https://canadianpharmacy-usa[.]net/product/contrave/\">buy contrave</a>\r\n
It's reassuring to know they task with respected manufacturers. A safe and
affordable privilege for managing my health.”
```

Fig 07. Castle’s honeypot forum is capturing an XRumer spam campaign promoting illicit pharmaceutical products.

Pivoting on this spam message, Castle's Research Team uncovered thousands of domains used by XRumer customers to push malicious ads. Upon further analysis of these posts, the following word cloud was produced, highlighting a significant portion of forum-related spam being associated with adult content such as drugs, pornography, or gambling.

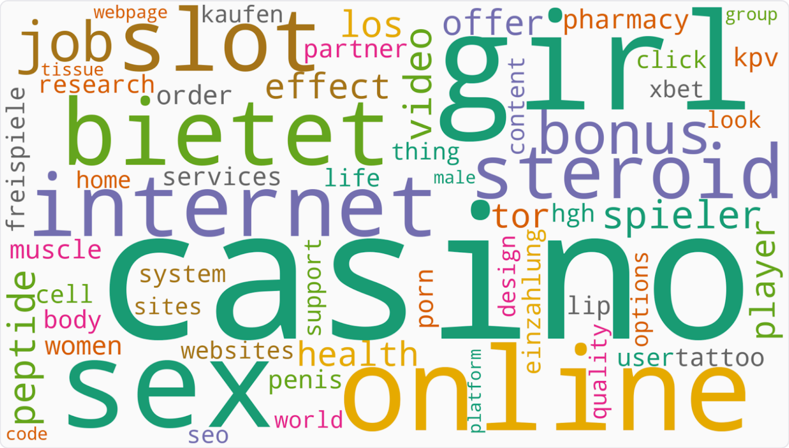
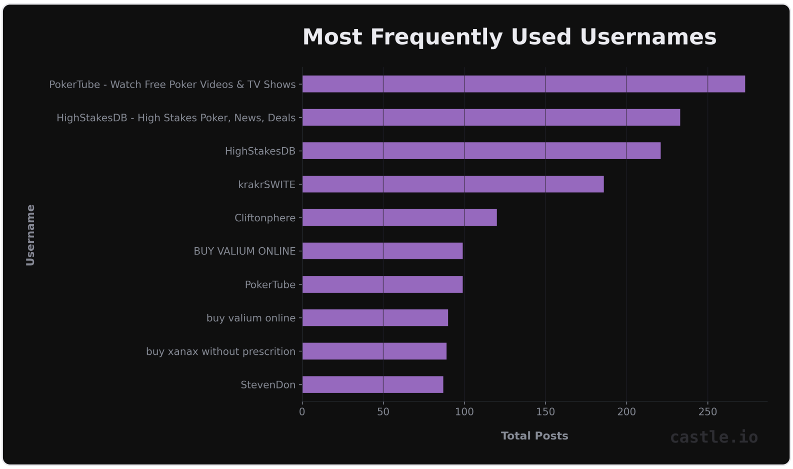
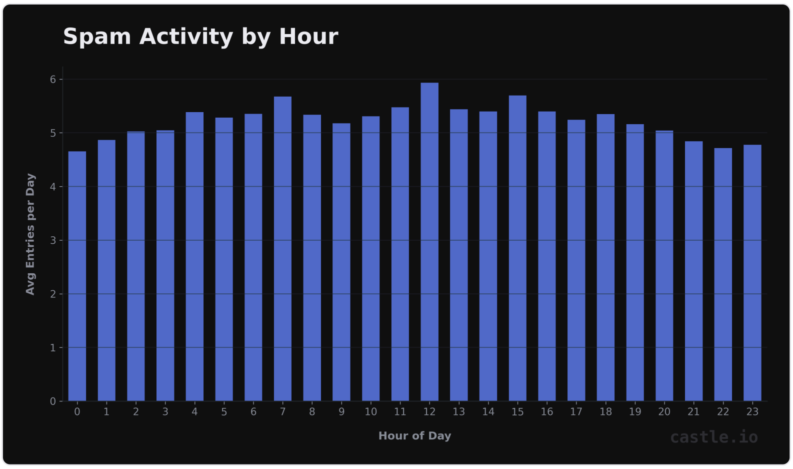


Fig 08. Word cloud of the most popular topics in forum spam campaigns.

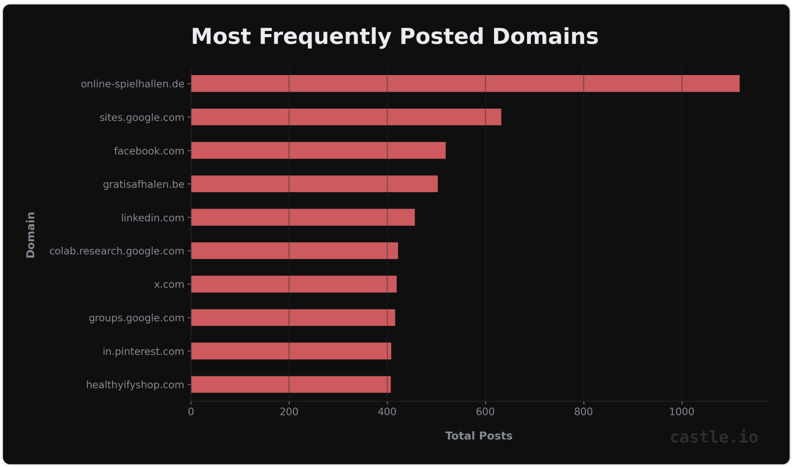
Further analysis of the dataset yields the following stats, showing a steady stream of spam throughout the day, across the week.



CAROUSEL_A Fig 09. Most frequently usernames used in spamming campaigns.



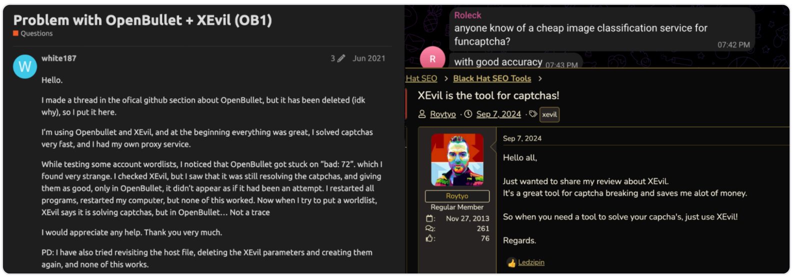
CAROUSEL_A Fig 10. Distribution of spam volume throughout the day.



CAROUSEL_A Fig 11. Most common domains embedded in spam content.

4. XEvil Analysis

To enable tools such as XRumer to register accounts, BotmasterLabs offers a dedicated CAPTCHA-solving tool that runs locally on the operator's machine. Castle’s Research Team notes that both individual operators of large-scale CAPTCHA-solving services, including 2Captcha, have widely adopted XEvil. Since 2017, XEvil has undergone continuous development, enabling users to solve CAPTCHA challenges from a wide range of providers, including reCAPTCHA, Arkose Labs (formerly known as FunCaptcha), and HCaptcha. As a result, XEvil has become a core component for actors engaged in large-scale botting operations.



Problem with OpenBullet + XEvil (OB1)
Questions

white187 3 Jun 2021

Hello.

I made a thread in the ofical github section about OpenBullet, but it has been deleted (idk why), so I put it here.

I’m using Openbullet and XEvil, and at the beginning everything was great, I solved captchas very fast, and I had my own proxy service.

While testing some account wordlists, I noticed that OpenBullet got stuck on “bad: 72”. which I found very strange. I checked XEvil, but I saw that it was still resolving the catpchas, and giving them as good, only in OpenBullet, it didn’t appear as if it had been an attempt. I restarted all programs, restarted my computer, but none of this worked. Now when I try to put a worldlist, XEvil says it is solving captchas, but in OpenBullet… Not a trace

I would appreciate any help. Thank you very much.

PD: I have also tried revisiting the host file, deleting the XEvil parameters and creating them again, and none of this works.

Roleck
anyone know of a cheap image classification service for funcaptcha? 07:42 PM
with good accuracy 07:43 PM

Hat SEO > Black Hat SEO Tools >

XEvil is the tool for captchas!
Roytyo · Sep 7, 2024 · xevil

Roytyo
Regular Member
Nov 27, 2013
261
76

Sep 7, 2024

Hello all,

Just wanted to share my review about XEvil.
It's a great tool for captcha breaking and saves me alot of money.

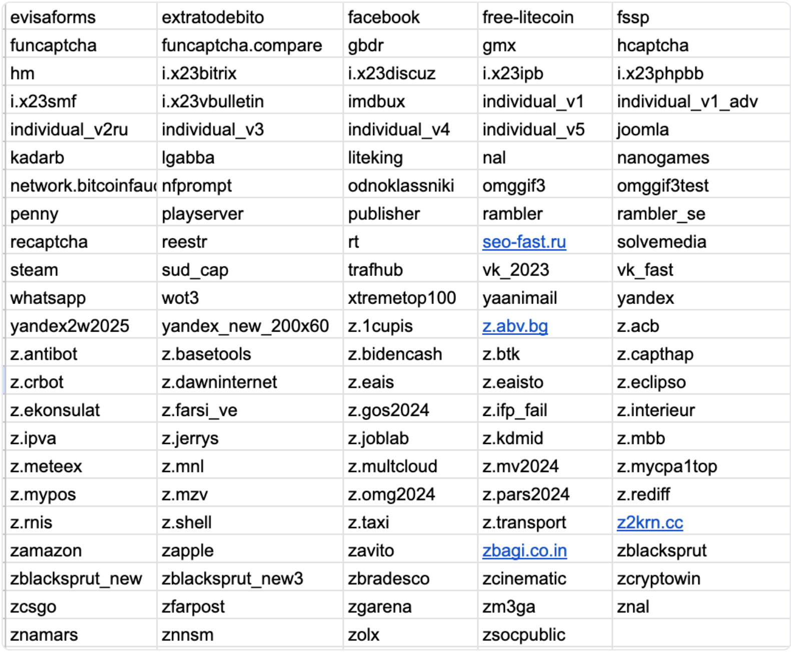
So when you need a tool to solve your capcha's, just use XEvil!

Regards.

Ledzipin

Fig 12. Online discussion of using XEvil

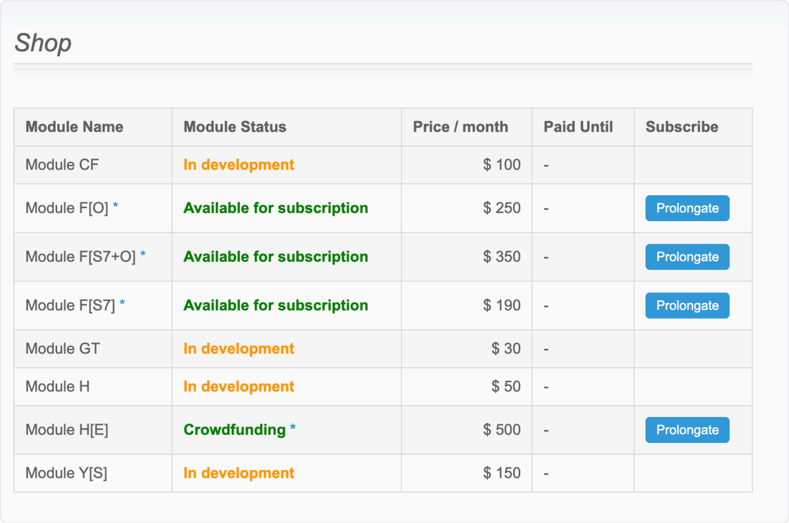
As of this report, XEvil 6.0 supports approximately 100 types of image CAPTCHA across multiple platforms. Targets include government websites and social media services, among others.



evisaforms	extratodebito	facebook	free-litecoin	fssp
funcaptcha	funcaptcha.compare	gbdr	gmx	hcaptcha
hm	i.x23bitrix	i.x23discuz	i.x23ipb	i.x23phpbb
i.x23smf	i.x23vbulletin	imdbux	individual_v1	individual_v1_adv
individual_v2ru	individual_v3	individual_v4	individual_v5	joomla
kadarb	lgabba	liteking	nal	nanogames
network.bitcoinfau	nfprompt	odnoklassniki	omggif3	omggif3test
penny	playserver	publisher	rambler	rambler_se
recaptcha	reestr	rt	seo-fast.ru	solvemedia
steam	sud_cap	trafhub	vk_2023	vk_fast
whatsapp	wot3	xtremetop100	yaanimail	yandex
yandex2w2025	yandex_new_200x60	z.1cupis	z.abv.bg	z.acb
z.antibot	z.basetools	z.bidencash	z.btk	z.capthap
z.crbot	z.dawninternet	z.eais	z.eaisto	z.eclipso
z.ekonsulat	z.farsi_ve	z.gos2024	z.ifp_fail	z.interieur
z.ipva	z.jerrys	z.joblab	z.kdmid	z.mbb
z.meteex	z.mnl	z.multcloud	z.mv2024	z.mycpa1top
z.mypos	z.mzv	z.omg2024	z.pars2024	z.rediff
z.rnis	z.shell	z.taxi	z.transport	z2krn.cc
zamazon	zapple	zavito	zbagi.co.in	zblacksprut
zblacksprut_new	zblacksprut_new3	zbradesco	zcinematic	zcryptowin
zcsgo	zfarpost	zgarena	zm3ga	znal
znamars	znnsm	zolx	zsocpublic	

Fig 13. Full list of targeted platforms and captchas.

XEvil customers are able to request custom plugins via the support forum, which has increased the tool's flexibility and adoption. Customers can also purchase model weights for specific CAPTCHA types through the XEvil marketplace, granting them access to more specialized site-specific CAPTCHAs.



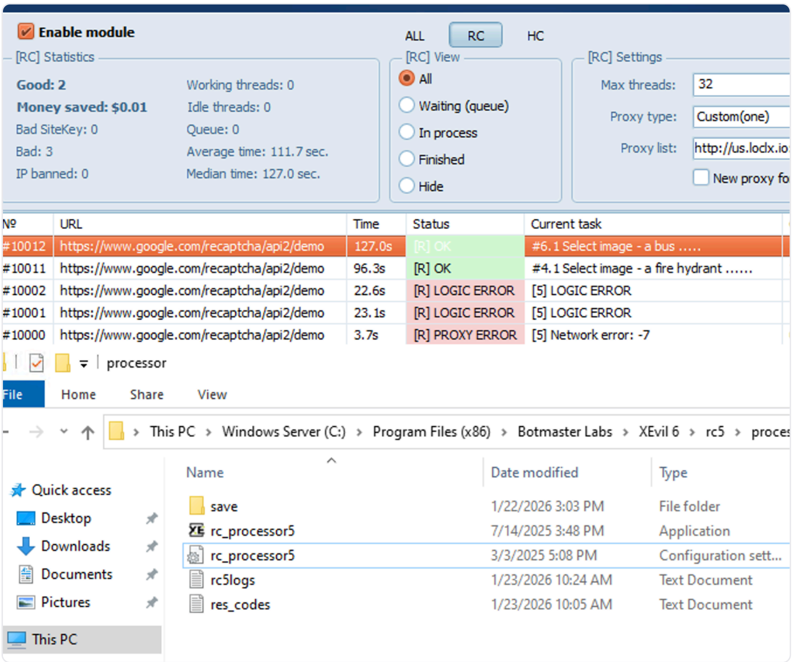
Shop

Module Name	Module Status	Price / month	Paid Until	Subscribe
Module CF	In development	$ 100	-	
Module F[O] *	Available for subscription	$ 250	-	Prolongate
Module F[S7+O] *	Available for subscription	$ 350	-	Prolongate
Module F[S7] *	Available for subscription	$ 190	-	Prolongate
Module GT	In development	$ 30	-	
Module H	In development	$ 50	-	
Module H[E]	Crowdfunding *	$ 500	-	Prolongate
Module Y[S]	In development	$ 150	-	

Fig 14. XEvil plugins system enabling users to bypass website specific CAPTCHAs. H=HCaptcha, F=FunCaptcha

4.0.1 XEvil's Headless Solver

XEvil's HCaptcha and reCAPTCHA solving library is implemented in the rc_processor5 module, a VMP-packed Delphi binary. The core logic uses the Chromium Embedded Framework to render and execute JavaScript, while XEvil uses an almost fully static browser fingerprint to simulate legitimate traffic.



☑ **Enable module**

[RC] Statistics

Good: 2
Money saved: $0.01
Bad SiteKey: 0
Bad: 3
IP banned: 0

Working threads: 0
Idle threads: 0
Queue: 0
Average time: 111.7 sec.
Median time: 127.0 sec.

[RC] View

● All
○ Waiting (queue)
○ In process
○ Finished
○ Hide

[RC] Settings

Max threads: 32
Proxy type: Custom(one)
Proxy list: http://us.lodx.io
□ New proxy fo

№	URL	Time	Status	Current task
#10012	https://www.google.com/recaptcha/api2/demo	127.0s	[R] OK	#6.1 Select image - a bus .....
#10011	https://www.google.com/recaptcha/api2/demo	96.3s	[R] OK	#4.1 Select image - a fire hydrant ......
#10002	https://www.google.com/recaptcha/api2/demo	22.6s	[R] LOGIC ERROR	[5] LOGIC ERROR
#10001	https://www.google.com/recaptcha/api2/demo	23.1s	[R] LOGIC ERROR	[5] LOGIC ERROR
#10000	https://www.google.com/recaptcha/api2/demo	3.7s	[R] PROXY ERROR	[5] Network error: -7

processor

This PC › Windows Server (C:) › Program Files (x86) › Botmaster Labs › XEvil 6 › rc5 › proces

Name	Date modified	Type
save	1/22/2026 3:03 PM	File folder
rc_processor5	7/14/2025 3:48 PM	Application
rc_processor5	3/3/2025 5:08 PM	Configuration sett...
rc5logs	1/23/2026 10:24 AM	Text Document
res_codes	1/23/2026 10:05 AM	Text Document

Fig 15. XEvils rc_processor5 module

XEvil does not enforce HTTPS, which allows interception of its traffic. Castle's Research Team was able to use this to inject custom JavaScript and identify parts of the injected browser fingerprint. XEvil notably lacks support for several standard Chromium APIs, including mediaCapabilities, clipboard, and permissions, allowing for detection due to mismatch from a standard Chrome browser. Although XEvil does allow setting a custom user agent, the implementation does not override JavaScript-specific values, further causing it to stand out.

Default XEvil user agent:

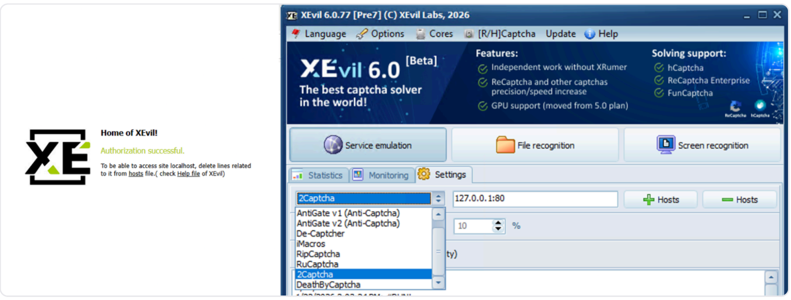
```
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
```

JavaScript Source	Value
navigator.vendor	"Google Inc."
navigator.vendorSub	""
navigator.product	"Gecko"
navigator.productSub	"20030107"
navigator.appName	"Netscape"
navigator.appCodeName	"Mozilla"
navigator.platform	"Win32"
navigator.language	"ru-RU"
navigator.deviceMemory	8
navigator.hardwareConcurrency	8
navigator.maxTouchPoints	0
navigator.cookieEnabled	true
navigator.doNotTrack	"1"
navigator.onLine	true
navigator.pdfViewerEnabled	false
navigator.webdriver	false
screen.availTop	0
screen.availLeft	0
screen.availHeight	1040
screen.availWidth	1920
screen.width	1920
screen.height	1080
screen.colorDepth	24
screen.pixelDepth	24

∗Note: Both screen.innerWidth and screen.innerHeight are randomized per session and are **not** static.

4.0.2 XEvil API

XEvil's adoption has been largely fueled by its compatibility with major CAPTCHA-solving services, which enable it to run locally and mimic APIs from services such as 2Captcha, AntiCaptcha, and Death By Captcha. This allows clients to easily swap out these larger services for XEvil, saving significant money by running it locally.



Home of XEvil!

Authorization successful.

To be able to access site localhost, delete lines related to it from hosts file.(check Help file of XEvil)

XEvil 6.0.77 [Pre7] (C) XEvil Labs, 2026

2Captcha

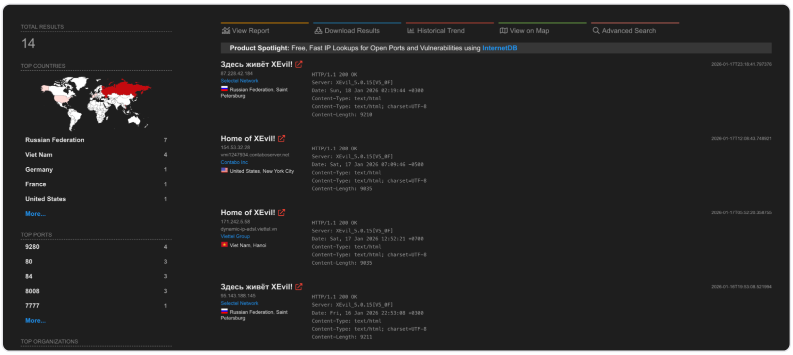
AntiGate v1 (Anti-Captcha)
AntiGate v2 (Anti-Captcha)
De-Captcher
iMacros
RipCaptcha
RuCaptcha
2Captcha
DeathByCaptcha

127.0.0.1:80

10 %

Fig 16. XEvil Webserver API.

A simple Shodan query yields a number of public-facing XEvil instances in Russia, the United States, and Vietnam. While most XEvil instances use proxies by default, this is not guaranteed, and Defenders are encouraged to block these IPs.



TOTAL RESULTS

14

TOP COUNTRIES

Russian Federation	7
Viet Nam	4
Germany	1
France	1
United States	1
More...	

TOP PORTS

9280	4
80	3
84	3
8008	3
7777	1
More...	

TOP ORGANIZATIONS

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

Здесь живёт XEvil!
87.228.42.184
Selectel Network
Russian Federation, Saint Petersburg

2026-01-17T23:18:41.797376

```
HTTP/1.1 200 OK
Server: XEvil_5.0.15[V5_0F]
Date: Sun, 18 Jan 2026 02:19:44 +0300
Content-Type: text/html
Content-Type: text/html; charset=UTF-8
Content-Length: 9210
```

Home of XEvil!
154.53.32.28
vmi1247934.contaboserver.net
Contabo Inc
United States, New York City

2026-01-17T12:08:43.748921

```
HTTP/1.1 200 OK
Server: XEvil_5.0.15[V5_0F]
Date: Sat, 17 Jan 2026 07:09:46 -0500
Content-Type: text/html
Content-Type: text/html; charset=UTF-8
Content-Length: 9035
```

Home of XEvil!
171.242.5.58
dynamic-ip-adsl.viettel.vn
Viettel Group
Viet Nam, Hanoi

2026-01-17T05:52:20.358755

```
HTTP/1.1 200 OK
Server: XEvil_5.0.15[V5_0F]
Date: Sat, 17 Jan 2026 12:52:21 +0700
Content-Type: text/html
Content-Type: text/html; charset=UTF-8
Content-Length: 9035
```

Здесь живёт XEvil!
95.143.188.145
Selectel Network
Russian Federation, Saint Petersburg

2026-01-16T19:53:08.521994

```
HTTP/1.1 200 OK
Server: XEvil_5.0.15[V5_0F]
Date: Fri, 16 Jan 2026 22:53:08 +0300
Content-Type: text/html
Content-Type: text/html; charset=UTF-8
Content-Length: 9211
```

Fig 17. Public facing XEvil instances. (Shodan)

5. Mitigation Strategies

- **Enforce hostname and URLs where possible**: Due to XEvil and other CAPTCHA solvers not loading the page submitted in the task, in some cases it's possible to detect a mismatch in the hostname returned by commercial CAPTCHA solvers.
- **Don't rely on image-based CAPTCHA as the only line of defense**: Organizations should use additional strong JavaScript signals alongside verification methods such as email and phone to drive up costs for bot operators.
- **Track challenge load times**: Because the CAPTCHA is loaded externally, the time between when the user viewed the form and when the CAPTCHA was loaded might differ. Organizations should check whether the `challenge_ts` is before or significantly after the page load time (`window.performance`); if so, the user should be blocked.

6. Observables

6.0.3 Network Observables

IP Address	Hosting Org	Country	Description
157[.]90[.]133[.]91:80	Hetzner Online GmbH	DE	Public-facing XEvil solving instance.
144[.]76[.]203[.]211:80	Hetzner Online GmbH	DE	Public-facing XEvil solving instance.
212[.]192[.]24[.]166:80	ITSOFT LLC	RU	Public-facing XEvil solving instance.
87[.]228[.]42[.]184:80	Selectel Network	RU	Public-facing XEvil solving instance.
147[.]135[.]255[.]209:80	OVH SAS	FR	Public-facing XEvil solving instance.
5[.]35[.]97[.]91:80	JSC IOT	RU	Public-facing XEvil solving instance.
212[.]192[.]24[.]133:80	ITSOFT LLC	RU	Public-facing XEvil solving instance.
109[.]194[.]67[.]56:80	CJSC ER-Telecom Holding Tver' branch	RU	Public-facing XEvil solving instance.
87[.]228[.]42[.]186:80	Selectel Network	RU	Public-facing XEvil solving instance.
154[.]53[.]32[.]28:80	Contabo Inc	US	Public-facing XEvil solving instance.
171[.]242[.]5[.]58:80	Viettel Group	VN	Public-facing XEvil solving instance.
95[.]143[.]188[.]145:80	Selectel Network	RU	Public-facing XEvil solving instance.
117[.]1[.]131[.]151:80	Viettel Group	VN	Public-facing XEvil solving instance.

Domain	Description
www[.]BotmasterLabs[.]net	BotmasterLabs English website
www[.]botmasterru[.]com	BotmasterLabs Russian website
www[.]XEvil[.]net	XEvil Website
botmastersupport[.]com	BotmasterLabs support forum
dwld[.]org	BotmasterLabs distribution website
fdc[.]xchecker[.]net	XRumer Proxy Checking Server

6.0.4 File Observables

Filename	SHA-256 Hash	Description
XEvil_5.0.15.866_Setup(RC_Fixed2024).exe	d648a2fe16caa290c3ead0b28fc4e6592f8ef5b12eff363dceebcc056c6408a3	XEvil 5.0 Setup File
rc_processor5.exe	20211e4db11fec6c0988224f376dacda8a1ca6e78f33c2151d62c2bef9e5919b	XEvil 5.0 CAPTCHA Solver Module
XEvil_6.0.77.1176_Setup.exe	4d24ee0dae17cb1702ac973430549b3f722c7da722631b71ce3bface4a621a6b	XEvil 6.0 Setup File
rc_processor5.exe	74a3a45e0e5358893d4e5f84e24d7168b4f243629ea2514bebe5c9b6b384cf48	XEvil 6.0 CAPTCHA Solver Module

7. Future Outlook

BotmasterLabs continues to actively develop XRumer and XEvil, with their next major release anticipated in the coming months. XRumer has significantly improved its auto-generated responses by integrating support for commercial machine learning models. Additionally, XEvil has undergone a major overhaul and is expected to introduce support for reCAPTCHA Enterprise, Cloudflare, SmartCaptcha, and GeeTest. Castle's Research Team assesses that both XEvil and XRumer will continue to support low-level cybercrime.

This trend indicates a broader shift within the automated abuse landscape. Threat actors are increasingly weaponizing artificial intelligence to bypass traditional security controls at scale. As machine learning models become more accessible and cost-effective for cybercriminals, the overall efficacy of image-based CAPTCHA is expected to continue to decline.

Consequently, organizations should pivot away from relying solely on static visual challenges. Defenders are advised to adopt multi-layered, behavior-based detection strategies. Implementing advanced device fingerprinting, biometric interaction analysis, and continuous session monitoring to counter automated threats such as XEvil and XRumer.